Presentation to the
Confidentiality, Privacy, and Security Workgroup
of the American Health Information Community
by
SureScripts, LLC
April 12, 2007

Thank you very much for the opportunity to provide testimony today with respect to health information exchanges, and in particular SureScripts, and respond to some of the questions posed by the Workgroup regarding privacy and security for this meeting. My name is Paul Uhrig, and I am the Executive Vice President of Corporate Development, General Counsel, and Chief Privacy Officer of SureScripts.

As a brief background on SureScripts, the company was founded in 2001 by the pharmacy industry through the National Association of Chain Drug Stores and the National Community Pharmacists Association -- the two trade associations that collectively represent the nation's chain and independent pharmacies. Our mission is to improve the overall prescribing process through the use of health IT, and to ensure, among other things, neutrality, patient safety, privacy and security, and freedom of choice of a patient's choice of pharmacy and a physician's choice of therapy. SureScripts has created and operates, on behalf of the pharmacy industry, an open, neutral, and secure information system, known as the Pharmacy Health Information Exchange.

The Company's initial services, sending and receiving electronic prescription transactions, were first put into production in January, 2004. Similar to the network that connects banks to Automated Teller Machines (ATMs), the Pharmacy Health Information Exchange seamlessly connects physicians with pharmacies on

a real time basis. The Pharmacy Health Information Exchange allows the secure, reliable transmission and delivery of electronic prescription information between computers at the pharmacy and computers at the physician's office. A complete and, since it is not handwritten, legible prescription can be sent from a prescriber's office to the pharmacy, all in seconds, even before the patient has left the physician's office, and the prescription could be waiting for the patient when she arrives at the pharmacy of her choice. SureScripts does not develop, sell, or endorse electronic prescribing software or applications; rather, we work with pharmacy and physician technology vendors to certify their prescribing systems for connection to the Pharmacy Health Information Exchange. We don't have a direct relationship with the patient; our relationship is with the providers who serve them.

While there are some variations on the model, the contracting structure is relatively straightforward. On the one hand, we contract with vendors of physician systems, whether stand alone e-prescribing systems or full functionality electronic medical record systems, so that those systems, when licensed and used by the properly authenticated physician, can communicate with pharmacies. On the other hand, we contract with pharmacies, either directly with respect to those that have their own proprietary systems, or pharmacy vendors who license their pharmacy management systems pharmacies. Today, more than 95 percent of the nation's retail pharmacies have tested and certified their pharmacy applications on the Pharmacy Health Information Exchange, and physician software vendors whose customer base represents over 150,000 prescribing physicians today have contracted with SureScripts, and most have completed the process of certifying their applications on the Pharmacy Health Information Exchange.

Accordingly, pharmacies and physicians who are contracted with, and connected to, SureScripts can exchange, in a real-time, secure, and HIPAA compliant manner, prescription messages such as new prescriptions, refill requests, and refill authorizations. All of these messages comply with the NCPDP SCRIPT Standard, which was the standard adopted by the Federal Government for e-prescribing transactions in the Medicare Modernization Act ("MMA"). As those of you who are familiar with the MMA know, there are many other e-prescribing messages that either have been declared as foundation standards by the Secretary, or which were evaluated and tested through the 2006 MMA pilot programs, including messages for medication history delivery.

With respect to electronic prescribing messages, such as new prescriptions and refill requests, the Pharmacy Health Information Exchange is available and in production in 49 states and the District of Columbia. The only reason that it is not available all 50 states is because one state has yet to adopt legislation that clears the way for e-prescribing.

In addition to the delivery of what I refer to as classic e-prescribing information (new prescriptions and refills), SureScripts is making drug benefit coverage information from payers and PBMs available to physicians in real time and at the point of care so that the most appropriate and cost-effective therapy can be prescribed. Finally, in certain limited markets, a patient's medication history, sourced from participating pharmacy's dispensed medication history records or payer/PBM records, can be made available, with patient consent, to the provider who is providing care to that patient. There is no better example of the need and value of robust medication history being available at the point of care than the experiences of Katrina Health. SureScripts had the honor of participating in the

government led program to make the medication history of Katrina evacuees available to providers of care, wherever those evacuees were ultimately relocated to. The benefits of such a program are proven, and are immeasurable in terms of lives saved and proper care given.

There is an increasing demand in the healthcare market place for medication history information to be provided electronically to hospitals so that they can comply with their JCAHO Medication Reconciliation requirements. As you know, JCAHO requires that hospitals conduct medication reconciliation upon admission and throughout the continuum of care. Today that is a time consuming, manual, and error prone task. In addition, many personal health record companies are seeking connectivity to pharmacy in order to pre-populate a patients' PHR with medication history and ease the burden on the patient having to manually input their medications. While we are evaluating both business and legal issues related to these models, except for our participation in an extremely limited and controlled NHIN-sponsored PHR project last year, we have not connected with entities for purposes of Medication Reconciliation or pre-population of PHRs.

Any information provided through the Pharmacy Health Information Exchange can be used for one purpose, and one purpose only, and that is the provision of healthcare to the patient. We have no right, and do not permit anyone who receives pharmacy information, to use it other than for the provision of care to the patient. Secondary uses are not allowed.

Given the sensitivity of handling prescription and patient medication history information, every entity that sends or transmits any personal or protected health information through the Pharmacy Health Information Exchange, from the

pharmacy to the prescriber, and back again, is either a covered entity as defined by HIPAA, or subject to a HIPAA compliant business associate agreement. SureScripts is a business associate of the pharmacies as well as others, and as such has agreed to comply with all of the HIPAA related requirements imposed on business associates relating to security, privacy, and confidentiality. We follow not only the HIPAA guidelines and requirements with respect to security measures, but other best practices with respect to the transmission and storage of PHI, including, but certainly not limited to, ensuring that all transmissions of personal health information are encrypted; using secure encrypted databases, redundancy and back-up procedures, audit trails, intrusion technology, and highly secure data facilities that require multiple levels of biometric identification to gain access. In addition, we have comprehensive policies relating to limited access to information, retention and destruction of information, use of laptops, strong passwords, etc. We also conduct annual third party audits to test our compliance and to ensure that we are maintaining best practices in the industry.

While we obviously believe that our systems are highly secure, we also have policies and procedures in the highly unlikely event that there is ever a breach of our security or PHI is mishandled in any way. An emergency response team is charged with responsibility for responding to any breach of security and taking the appropriate steps to mitigate any harm, especially harm to those whose information may have been compromised. These policies include complying with any applicable state notification laws, working with our partners and covered entities to inform them and patients of a breach, as well as working with law enforcement, all as the particular circumstances require. We also have a designated privacy officer and a security officer, as well as an internal committee dedicated to security procedures. The security committee is made up not only of internal SureScripts

personnel, but also the security personnel of the major chain pharmacies who provide information through the Pharmacy Health Information Exchange.

We do have a standard HIPAA Business Associate Agreement that we require all who provide or receive information, or have access to information, to sign and comply with – often, however, covered entities request that we use their form of HIPAA BA agreement. Fortunately, most of the BA Agreements follow a common theme and have requirements that, although not always identical, are at least somewhat similar. Is it a burden to manage the various contracts – yes – would we prefer more uniformity – yes, but it is, for now, a manageable contract management and internal process to ensure that we are compliant with the various agreements and policies to which we are subject.

We implement these policies and procedures for many reasons - contracts impose these obligations on us, we adhere with a multitude of statutory and state common laws that govern privacy, we publicly state, as so many do about their own businesses, because it is important to do so, that we are HIPAA compliant -- but also both we and our partners, those who use the Pharmacy Health Information Exchange, fully understand the public trust that is necessary in order for the proper exchange of health information to occur. A breach of that trust would be devastating to the Company, not just because of legal liability issues, but the harm to reputation and business would adversely affect not only the Company and, in our case, the pharmacy industry, but also the health care industry and the deployment of health IT in general.

HIPAA obviously contemplated the electronic exchange of information – that is not new. I believe a reasonable debate can and should occur as to whether, when

the HIPAA rule was promulgated, anyone could have foreseen the deployment of health information exchanges as is occurring today, whether vertically based by industry, such as the Pharmacy Health Information Exchange, or regionally based, such as the RHIO's and other regional exchanges that are in development throughout the country, and the issues that arise from that deployment. However, it is not as easy as merely saying today that a certain type of entity that now "touches" the NHIN, especially a non-provider, is now and hereafter a covered entity.

HIPAA today treats covered entities differently depending upon their nature. Accordingly, whether other entities should be considered covered entities, and the requirements imposed upon them, requires a balancing of the important privacy and security needs against the role and function of the entity being regulated, and proper and legitimate use of the data. The focus of any requirements should be on one, the security of information, two, the proper use of information, three, accountability for disclosures, and four, vigorous enforcement of penalties against those who fail to properly secure the information or those who misuse the information, based upon clear rules. And we would suggest that today's world in which enforcement (and by this I mean private enforcement) is dependent on an increasingly lengthy chain of various, and perhaps inconsistent, business associate agreements, enforceable only by the parties to those agreements, may not create the trust in the system that is necessary for success. Our contracts will always address the use of data and the security of data; and while we would vigorously pursue anyone who breaches those agreements, one can legitimately question whether as a matter of public policy that is sufficient.

Having some entities covered by federal law, and others not, within the chain of custody of PHI does create ambiguity and complexity in areas that should be devoid of ambiguity and complexity. Some provisions of HIPAA may not be as relevant to health information exchanges as they are to providers, for instance, such as the requirement to provide a privacy notice to patients, and perhaps there are new requirements that should be imposed as we look at today's world and the future. Since today we as a Company comply with the privacy and security requirements of HIPAA that are imposed upon us by BA Agreements as a minimum standard, it would not be an undue burden if those same requirements were imposed upon us directly by HIPAA, but any additional requirements must be rationally related to the function and services of the entity being regulated.

The current debate around privacy and confidentiality is critical as we move from an anachronistic paper based system, that has its own privacy and security issues, to an electronic based system that will no doubt improve care and lead to healthier population, but that raises legitimate privacy concerns that require careful and reasoned debate and resolution. We appreciate being part of the process, and I look forward to your questions.